Senior Service College Fellowship

Civilian Research Project

SOCIAL MEDIA – DOD'S GREATEST INFORMATION SHARING TOOL OR WEAKEST SECURITY LINK?

BY

LIEUTENTANT COLONEL SUSAN CAMORODA
United States Army National Guard

USAWC CLASS OF 2010

U.S. Army War College, Carlisle Barracks, PA 17013-5050

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-04-2010	Civilian Research Paper	August 2009-April 2010

4. TITLE AND SUBTITLE

Social Media – DoD's greatest information sharing tool or weakest security link?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LTC Susan Camoroda

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Carnegie Mellon University/Heinz College
5000 Forbes Avenue
Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION A: UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This paper will consider the current use of Social Media in the Department of Defense (DoD): review current policies, review current use of this medium by DoD, and analyze the impact of a new DoD Directive regarding use of Social Media on military networks.
Social Media include many that are used primarily for distributing what is referred to as Strategic Communications (or Public Affairs Office/PAO) information - Facebook, Twitter, and various milblogs are examples. Other Social Media can be defined as Information Sharing portals – Army Knowledge Online, unit home pages, and DefenseLink.mil being three prime examples.
There are two overarching concerns with the use of Social Media - particularly Facebook and Twitter: Operations Security (OPSEC) and network security (or the perceived increase in risk to the DoD network through exposure to these commercial sites).
This paper will review the current policies regarding Social Media use in DoD and
provide an analysis regarding the appropriateness and effectiveness of these policies in securing the information network.

15. SUBJECT TERMS

Social media, information security, information sharing

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	40	

USAWC CIVILIAN RESEARCH PROJECT

SOCIAL MEDIA – DOD'S GREATEST INFORMATION SHARING TOOL OR WEAKEST SECURITY LINK?

by

Lieutenant Colonel Susan Camoroda
United States Army National Guard

Dr Rahul Telang
Project Advisor
Carnegie Mellon University, Heinz College

Dr Thomas McManus
United States Army War College Adviser

Disclaimer

US Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Susan Camoroda

TITLE: Social Media – DoD's greatest information sharing tool or weakest security link?

FORMAT: Civilian Research Project

DATE: 15 April 2010 WORD COUNT: 6,622 PAGES: 40

KEY TERMS: social media, information security, information sharing

CLASSIFICATION: Unclassified

This paper will consider the current use of Social Media in the Department of Defense (DoD): review current policies, review current use of this medium by DoD, and analyze the impact of a new DoD Directive regarding use of Social Media on military networks.

Social Media include many that are used primarily for distributing what is referred to as Strategic Communications (or Public Affairs Office/PAO) information - Facebook, Twitter, and various milblogs are examples. Other Social Media can be defined as Information Sharing portals – Army Knowledge Online, unit home pages, and DefenseLink.mil being three prime examples. There are two overarching concerns with the use of Social Media - particularly Facebook and Twitter: Operations Security (OPSEC) and network security (or the perceived increase in risk to the DoD network through exposure to these commercial sites).

This paper will review the current policies regarding Social Media use in DoD and provide an analysis regarding the appropriateness and effectiveness of these policies in securing the information network.

TABLE OF CONTENTS

SOCIAL MEDIA – DOD'S GREATEST INFORMATION SHARING TOOL OR WEAKEST SECURITY LINK?

Introduction

For many years there has been continual debate regarding the security of, and access to, the Department of Defense's Global Information Grid (DoD GIG). Some advocate denying all access to the internet from official military systems, others advocate limited access to a selected set of users and a specific set of commercial web sites, while a third group advocates open access to all – and there is a range of opinions and exceptions within these three groups. This ongoing debate has intensified recently due to the increased use of Social Networking Services (SNS), often called social media, emerging media, or new media. The Department of Defense (DoD) has chosen a different term – Internet Based Capabilities[1] - to refer to these tools. The term social media will be used throughout this paper to describe the services that have been discussed most adamantly as increasing the security risk to the GIG. These social media services are: Facebook, Twitter, Flickr, YouTube, Wikipedia, and blogs. Over the past year (2009), the DoD has been reviewing the use of, access to, and impact on both the information network and the work environment (productivity) of these social media services. The Office of the Secretary of Defense (OSD) and each separate service within the Department – Army, Navy, Air Force, and Marines – developed their own policies in the interim prior to the release of the DoD Directive Type Memorandum (DTM) on February 25, 2010. These interim policies ranged from deny all access (Marines)[2] to allowing unlimited access (Army) until an official DoD wide policy[3] is released. Each was different and caused confusion among the administrators, the

users, the public (families, friends and supporters of the military service member), and other civilian and government agencies that work with the different services. The varied policies also caused confusion internally within the services, the senior leadership, and the individual military members who were expected to adhere to these policies. For example, is a Marine who is assigned to an Army installation and unit allowed to use social media services? Strict adherence to Marine policy states no, while Army policy states yes. It was also unclear to many if the restrictions applied only to the official military systems or extended to personal home use. It became quickly apparent that the lack of an official, clear, Department-wide policy was becoming both a personnel and a public relations issue.[4]

A secondary question is the role of government developed social media tools used internally for collaboration, such as the Intelligence community's Intellilink (a version of Wikipedia), Analytic Space (A-Space, a 'Facebook for Spies'[5]), and milSuite[6]. These tools have been developed based on commercial designs, but are behind the GIG firewall, and thus (in theory) not as vulnerable to infiltration and other security concerns as are the commercial social media sites. Since these sites are password protected and access must be vetted and approved by a controlling authority, the audience is limited to those who are granted a certain level of 'trust' by being a member of the larger government community. This trust relationship is at the heart of the uncertainty surrounding the opening up of DoD networks to commercial social media. But with both types of social media tools (civilian and government), there is the overarching debate over the usefulness and appropriateness of these networking and collaboration tools in the performance of the DoD's missions.

This paper will consider the use of commercial social media in the Department of Defense through: review of current network security and operational security (OPSEC) policies to determine the adequacy of these documents to respond to any additional threat or risk to the GIG; review of current use of social media tools within the DoD prior to a final, official DoD policy; review of the expected impact of the recently released DoD DTM[7] and supplementing service memorandums[8] regarding use of Internet-based capabilities (social media) on military networks; and finally, provide recommendations on how to strengthen network defense by coordinating security policy implementation and emphasizing user responsibility at all levels.

Background

The Department of Defense is subject to continuous network probing by those seeking to infiltrate in order to obtain information regarding military plans, operations, policies and personnel. According to one report, the Department of Homeland Security and the Department of Defense "reported 5,488 *known* breaches to U.S. Government computers, and 54,640 incidents of malicious cyber activity against the Department of Defense alone in 2008."[9] Additionally, information regarding the design of an advanced military aircraft, the Joint Strike Fighter, was recently obtained by intrusions into a U.S. Defense Contractor's network.[10] These and many other breaches, intrusions, probes, and attacks are conducted daily. These successful infiltrations occur despite numerous Federal Government and Department of Defense Information and Network policies, Information Security training requirements, Information Security certification requirements, and various agencies and offices within the Federal Government and DoD dedicated to *ensuring* the GIG is secure (i.e. - U.S Strategic Command

(USSTRATCOM), Joint Task Force – Global Network Operations (JTF-GNO), Defense Information Systems Agency (DISA) and each of the service Chief Information Officers (CIOs), to name a few).

Incidents of cyber attack to DoD information networks occurred long before the advent and introduction of social media services. Of common knowledge are attacks through email systems using techniques known as social engineering or 'Phishing'. When successful, these attacks install malicious software (malware), Trojans, spyware or worms into the network. Information Assurance training and education has been an annual requirement for military information systems users (this includes all civilians and military personnel with access to and use of a military computer) for a number of years.[11] Despite this training, and despite publication in reports (in classified, unclassified and open source documents) of these attacks on a regular, almost daily basis, failure on the part of the Information Technology administrator or the Information Systems user to adhere to the standards or training is the common cause of most successful attacks.[12]

U.S. military personnel use commercial social media tools to communicate with friends and family others while deployed or simply away from 'home', while others use Web Logs (blogging) to tell their stories to the world at large. Many times soldiers and families feel that their 'First Amendment right' of freedom of speech is somehow violated when the use of social media tools is banned or restricted.[13] This clouds the discussion, though it is an issue that must be addressed, particularly in this time of two wars and thousands of soldiers deployed, fighting for what their family members and the public at large believe are all the rights of American citizens.[14] Consequences of a complete ban

on social media tools may result in negative impact on the recruitment and retention of the most important element of the military – its people. Or, if nothing else, bad public relations at a time when the military leadership requires the continued support of the American people.

Definition of Social Media

There are many definitions for social media (aka social networking, social software, emerging media, new media). For the purposes of this paper, social media refers to "an umbrella concept that describes social software and social networking – social software refers to various, loosely connected types of applications that allow individuals to communicate with one another, and to track discussions across the web as they happen".[15] In the Department of Defense, the social media used most prevalently are Facebook, Twitter, Flickr, and YouTube. It is these outward facing, public internet, commercial tools that are of concern and will be discussed in this paper.

Other social media tools used within the DoD GIG are used for collaboration in day-to-day operations. Some of these tools are Intellilink (a form of Wikipedia), 'A-Space' (Analytic Space used in the Intelligence Community), and Web Logs (blogs). The Army has developed its own suite of tools called 'milSuite'[16] which contains features that attempt to replicate the commercial software look, feel and function: milWiki (Wikipedia), milBlog (blogs), and milBook (Facebook). These tools are advertised as "offering users an opportunity to learn, share and connect with the AKO/DKO[17] community". Each of these tools enables information sharing, collaboration, 'crowd-sourcing', and the ability to reach and share information to build awareness and understanding with those outside of the immediate work environment and usual

information channels. This is ‘networking’ in the professional sense, and not subject to the same negative connotation of ‘social’ networking given to the commercial social media tools that are believed to be a security risk to the military networks (the GIG).

Open Government Initiative

In January 2009, President Obama signed the Open Government Initiative. This initiative informed the Federal Departments and Agencies that they were required to start thinking of new ways to conduct operations. Three main points were detailed in the initiative[18]:

- *Government should be transparent* – Transparency promotes accountability and provides citizens information about what government is doing
- *Government should be participatory* – Engage the public in policy-making discussions and open dialogs for ideas regarding ways to improve government operations
- *Government should be collaborative* – Engage the American public in the workings of their government. Collaboration and information sharing among federal departments and agencies, as well as other non-government agencies and the private sector in order to improve services, respond to crises, solicit feedback and improve partnerships

The intent of this initiative is to harness and use new technology (social media tools being part of the new technology) to share information between the Federal government and the citizens it serves, to seek input, and to engage in an open and continuous dialog. The Department of Defense, of course, is an element of the Federal government, and therefore, must comply with this initiative. Open discussions, seeking input, and continuous dialog are new concepts to the DoD, an organization that traditionally communicates through media releases, with the only ‘dialog’ being question and answer periods following a news conference or an official interview.

On December 8, 2009, the Open Government Directive was released. This document directed "executive departments and agencies to take specific actions to implement the principles of transparency, participation and collaboration set forth in the President's memorandum".[19] The Directive set milestones and timelines to develop a plan on how each was to enable a more open and collaborative environment in their respective agencies. A review of Federal department web sites shows that many have chosen social media tools that are popular, familiar, and easily accessible to the public as a starting point.[20] As a reference point, the following shows the use of Twitter and Facebook by the Department of Defense and the number of 'followers' as a gauge of interest in obtaining information from these agencies (data taken from the 'Official Department page' as of the date shown in 2010):

Agency	Twitter (Feb 24)	Facebook (Feb 22)
DoD	3,794	20,160
Chairman, Joint Chiefs of Staff	16,463	8,824
Army	25,216	170,854
Navy	8,725	81,667
Air Force	8,269	34,101
Marines	7,622	7,162
National Guard[21]	3,743	6,847
State Department	14,443	31,671

The need to meet the timelines implied in the Open Government Initiative and detailed in the Open Government Directive required the DoD to begin utilizing these tools before an official social media use policy could be finalized. In the interim, some services

embraced its use, while others denied access from official military networks due to uncertainty and the perceived level of risk regarding network and operational security vulnerabilities. Thus, in the absence of formal guidance, some senior leaders took the initiative. The Chief, National Guard Bureau is one who has embraced the use of social media and has written about its importance:

> *My first exposure to Twitter, a "micro-blogging" service, happened in Europe at our State Partnership Program conference. The conference chair opened with an announcement about the conference hash tag for Twitter. I had no idea what he was talking about, but several attendees did. Those attendees pointedly told me the information was useless to National Guard members since our networks blocked access to Twitter. Well, we fixed that problem, and I began to learn more about this new phenomenon and its potential impact on how we communicate.*
>
> *I use it to stress important messages to the National Guard community. Issues such as the importance of flu vaccines or National Preparedness Month can be highlighted to a broader audience. I also retweet stories from other senior Defense leaders and organizations to help them spread their core messages*.
>
> *The technology folks also worry about security of the network from attack — also a valid concern. But my response is: "Figure it out." These tools are too important to lock away. Some of the brightest minds in the country are focused on securing our networks and lowering this risk. I am confident they have the skills to both empower users and protect critical systems and data*.[22]

Information Sharing and the Need for Increased Collaboration

The 9/11 Commission Report issued in July 2004 drove home the fact that information is not always shared across the organizational boundaries of the separate governmental agencies. The development and slow implementation of internal government information sharing and collaboration policies resulted. The *National Strategy for Information Sharing* was released in October 2007 -six years after 9/11 and two years after Hurricane Katrina.[23] This document directs government agencies to focus their efforts on information sharing within the federal government, and also down

to the state, local, tribal and sometimes private sector critical infrastructure sector entities:[24]

> *For the past six years, this Administration has worked within the Federal Government, and with our State, local, tribal, private sector and foreign partners to transform our policies, processes, procedures, and – most importantly – our workplace cultures to reinforce the imperative of improved information sharing. The exchange of information should be the rule, not the exception, in our efforts to combat the terrorist threat.*

This document spawned supplementary, lower level documents that provided additional specificity regarding information sharing goals, techniques, expectations, management, and training. Some of these documents include:

- Department or Defense Information Sharing Strategy[25] - Four goals are outlined
    - Promote, encourage, and incentivize sharing
    - Achieve an extended enterprise
    - Strengthen agility in order to accommodate unanticipated partners and events
    - Ensure trust across organizations
- United States Intelligence Community Information Sharing Strategy[26] - A central principle is the recognition that information sharing is a **behavior** and not a technology
- Department of Homeland Security Information Sharing Strategy[27] - written to correct the interagency information sharing failures documented by the 9/11 Commission and Hurricane Katrina reports

These three strategies took the mandates from the National Strategy and developed details to guide their separate departments regarding information sharing internally within, and external to their own organization. 9/11, Hurricane Katrina, and other recent national disasters have proven that the development and institutionalization of

information sharing and collaborative tactics, techniques and procedures must be in place and practiced prior to the event occurring.

Network Security and Information Assurance Policies

Figure 1. On Cyber Patrol Training cartoon

A chart developed by the Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance (DASD(CIIA))[28] that accompanies the DASD(CIIA) Strategy[29] lists over 190 separate laws, strategies and policies, a number that does not include the various OPLANS (Operations Plans) and CONPLANS (Contingency Plans) of USSTRATCOM (U.S Strategic Command[30]).

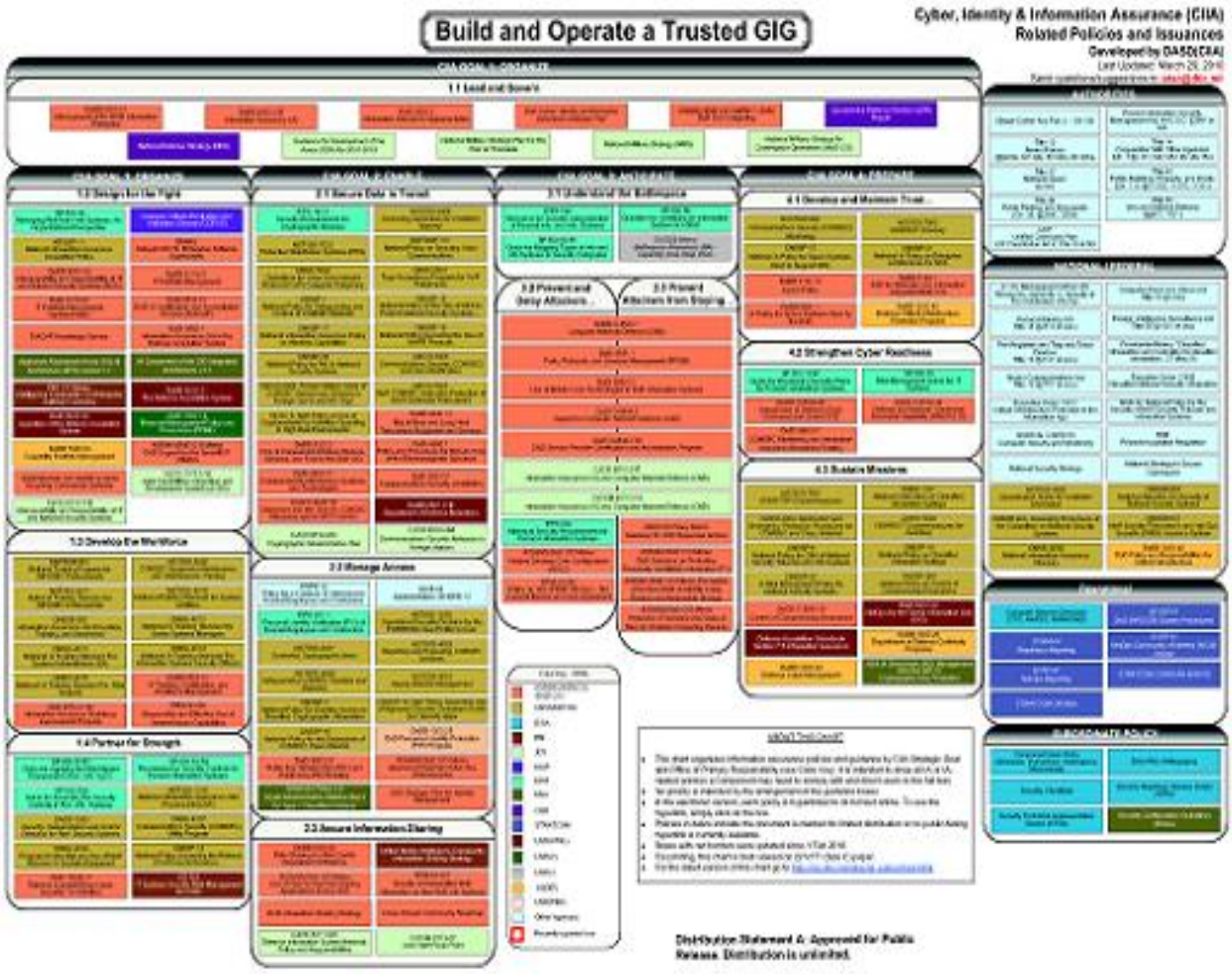

Figure 2. DASD(CIIA) Related Policies chart

This comprehensive chart provides a view of the myriad of applicable policies DoD agencies must adhere to in building, operating and securing the GIG.[31] The DASD(CIIA) Strategy "sets forth to support the DoD vision of freedom of action in cyberspace where:

- DoD missions and operations continue under any cyber situation or condition
- The cyber components of DoD weapons systems and other defense platforms perform only as expected
- DoD Cyber assets collectively, consistently, and effectively act in their own defense

- The Department has ready access to its information and command and control channels and its adversaries do not
- The Department of Defense information enterprise securely and seamlessly extends to mission partners"[32]

A review of this chart reveals it is not all inclusive. Missing are the separate service regulations that further define the steps the information system network and security managers must adhere to in order to comply with these higher level requirements. For example, Army Regulation 25-2, *Information Management / Information Assurance*[33] refers back to Department of Defense Directive 8750.01, *Information Assurance Training, Certification and Workforce Management*[34], providing additional detail and amplification, and

> "*assigns responsibilities for all Headquarters, Department of the Army (HQDA) staff, commanders, directors, IA personnel, users, and developers for achieving acceptable levels of IA in the engineering, implementation, operation, and maintenance (EIO&M) for all information systems (ISs) across the U.S. Army Enterprise Infostructure*."[35]

The questions become: With all these policies, how is it that the Department of Defense's military information systems networks are still being infiltrated, and sensitive military information is still being stolen? Is it impossible to secure the information systems 100%? Are risks being taken? Are these risks at an unacceptable level? Does DoD need to completely isolate it's networks from the internet? Would this mean the 'terrorists' (cybercriminals, hackers, etc) have won?

Information Systems Certification – Hardware and Software

Department of Defense Directive 8510.01 (DODD 8510.01)[36] specifies the processes necessary to accredit an information system (any piece of hardware ranging from server to workstation) prior to it being connected to the GIG. These standards are

detailed, and numerous layers of management are assigned the responsibility to ensure these accreditation standards are met, reviewed, renewed and followed. This Directive interprets and amplifies for DoD the laws set forth in U.S Code, commonly known as the Federal Information Security Management Act (FISMA) of 2002.[37] The standards are very straightforward, detailing what is expected and who is responsible.

"The head of each agency shall be responsible for:[38]

- providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification or destruction
- ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control including
    - implementing policies and procedures to cost-effectively reduce risks to an acceptable level
    - periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented
- ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards and guidelines
- ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions"

As stated, each service then develops a policy based on the higher level authority to provide further detail and guidance to their own personnel. For example, the Army has three publications which discuss Information Assurance requirements:[39]

- Army Regulation 25-2, *Army Knowledge Management and Information Technology*
- Army Regulation 25-2, *Information Assurance*
- Army Regulation 380-53, *Information Systems Security Monitoring*

Another standard, this one pertaining to software, is the Federal Desktop Core

Configuration. In 2006, the U.S. Air Force, in partnership with Microsoft, developed what they called the 'Standard Desktop Configuration'[40] in order to support their information security and information management efforts. After successful deployment of these standards across their 435,000 desktops and laptops, with the main feature being the disabling of 'System Administration' capability from all users except for legitimate System Administrators, the Air Force shared their initiative with the other services. This initiative was such a success that the DoD, Army, Navy and Marines all adopted these standards. A 'good idea' is good to continue to share, so in 2007, the Office of Management and Budget adopted these standards and made them mandatory across all Federal Departments and Agencies. The memorandum is titled "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems".[41] The standards are applicable to all information systems using Microsoft XP and Vista, Internet Explorer and Microsoft Office, and must be considered in the acquisition of any new products.[42] The development of these standards was in collaboration with the National Institutes of Technology (NIST), DoD, and the Department of Homeland Security (DHS). An outside observer would assume that all this coordination, effort and acceptance of these standards would help solve the network security problem. The OMB Mandate states[43]

> *DoD has worked with NIST and DHS to reach a consensus agreement on secure configurations of the Vista™ operating system, and to deploy standard secure desk tops for Windows XP™. Information is more secure, overall network performance is improved, and overall operating costs are lower.*

Apparently the FDCC was not the final solution. The Air Force has recently contracted with private industry for a $9.7 million dollar Host Based Security System (HBSS)[44] that will also be deployed throughout the GIG. Some of the benefits of this system are:

- Built on McAfees's Host Intrusion Protection System
- Will be deployed on over 5 million desktops, laptops, notebooks, and servers
- Is the first and last line of defense – provides 360 degree protection
- A 'game-changer' in terms of virus protection

With all these promises, it could be assumed that the DoD/GIG network security problem is solved – ready for any and all forms of attack. Unfortunately, these same promises are made over and over with each new information security software deployment. Only time will tell.

Unfortunately, all of these standards cannot seem to stop network security breaches. Risk to the GIG with social media tools is no greater than inappropriate use of hardware. Examples of inappropriate use of hardware are two recent events regarding the use of USB devices which has caused a ban to be placed on these items until further guidance is developed. These examples are: USB devices containing worms and malware being used to transfer information from Secure (SIPRnet) systems to nonsecure (NIPRnet) systems[45], and USBs containing sensitive military information found to be for sale at Afghan bazaars.[46] In both examples, it is the user (individual) who caused the insecurity, not the information system. Failure to properly use and maintain control of hardware is the cause of these insecurities.

Figure 3. On Cyber Patrol training cartoon – USB drives[47]

Another problem occurs with the banning of the use of USB devices – Commanders still order their subordinates to 'get me that information now', causing the subordinate to 'work around' the security rules, up to and including emailing the information to an unsecured account – such as 'gmail' states Richard Ford, Computer Science Professor of Assured Information at Florida Institute of Technology.[48] For policies and procedures to be successful, people must adhere to them.

Network Administrator Training and Requirements

DoD Directive 8570.01, Information Assurance Training, Certification and Workforce Management, details the requirements for all personnel who use military systems at all levels - from systems administrators to users. The Directive states that:

- All authorized users of DoD Information Systems (IS) shall receive initial Information Assurance (IA) orientation as a condition of access and thereafter must complete annual IA refresher training
- Privileged users and IA managers shall be fully qualified, trained and certified to DoD baseline requirements to perform their IA duties
- Personnel performing IA privileged user or management functions, regardless of job series or military specialty, shall be properly identified in the DoD Component personnel databases

- All IA personnel shall be identified, tracked and managed so that IA positions are staffed with personnel trained and certified by category, level and function
- All positions involved in the performance of IA functions shall be identified in appropriate manpower databases by category and level
- The status of the DoD Component IA certification and training shall be monitored and reported as an element of mission readiness and as a management review item[49]

DoD Directive 8570.01E is an overarching document. More specific guidance regarding specific training and certification requirements at each level of use and function is detailed in DoD Manual 8570.01-M.[50] Three main points emphasize that IA personnel must be properly trained, and managers must:

- Implement a formal IA workforce skill development and sustainment process, compromised of resident course, distributive learning, blended training, supervised on the job training (OJT), exercises and certification/recertification
- Verify IA workforce knowledge and skills through standard certification testing
- Augment and expand on a continuous basis the knowledge and skills obtained through experience or formal education

So, what is lacking in these policies? What is missing that is allowing an increasing number of network intrusions? Is it a lack of policies to cover each type of incident, or is it a failure on the part of the personnel implementing the policies? Is it a lack of skill, training, adherence to security requirements in the DoD workforce, or is it that there are so many policies, so many different types of hardware and software, and so many ways the 'black hats' (bad guys) can stay ahead in the various ways they devise to introduce malware, Trojans or exploit the network through spear phishing attacks, that result in so much probing of, and successful attacks on, the GIG?

User Level Training

There are two main elements to user level training: training regarding the standards of use of the hardware and software assigned, and training on Operational Security (OPSEC) with respect to the information posted and shared over military information systems. Both of these are of major concern when discussing the use of social media on the GIG. OPSEC is also a concern over any communication medium – personal, telephone, letter, email, and social media – by members of the DoD. The old World War II adage of 'loose lips sink ships' is still applicable today, and social media is just the latest form of communications technology that require personal diligence in its use.

As stated above, DoD Manual 8570.01E mandates "all authorized users of DoD IS shall receive initial IA awareness orientation as a condition of access and thereafter must complete annual IA refresher training".[51] DoD Manual 8570.01-M, Chapter 6 states in great detail the user level training requirements, to include:[52]

- Examples of external threats such as script kiddies, crackers, hackers, protesters, or agents in the employ of terrorist groups or foreign countries
- Authorized user risk from social engineering
- Knowledge of malicious code (i.e. logic bomb, Trojan horse, malicious mobile code, viruses, and worms) including how they attack, how they damage an IS, how they may be introduced inadvertently and/or intentionally, and how users can mitigate their impact
- How to prevent self-inflicted damage to system information security through disciplined application of IA procedures such as proper logon, use of passwords, preventing spillage of classified information, e-mail security, etc
- Embedded software and hardware vulnerabilities, how the DoD corrects them (e.g. IAVA[53] process) and the impact on the authorized user

Again, it appears that the IA rules and requirements are well defined and detailed. So, why are so many insecurities caused by user failure to adhere to and implement the training received? Some believe the blame lies directly with the human factor influences at all levels:

> *The end user – the service member or Pentagon civilian sitting at his desktop - is largely responsible for letting in these electronic intruders. They're the ones who set passwords to "1234", plug unknown drives into their computer, or download a Trojan virus when all they meant to do was sneak a peek at some online porn. "This makes us our own worst threat", writes one DoD network security specialist. "There are a variety of reasons for this and most are tied to the collective DoD inability to mitigate known vulnerabilities – vulnerabilities users intentionally and unintentionally utilize to create adverse impacts or risks".*
>
> *The Pentagon spends millions of dollars every year on so-called "information assurance" – checking to see that military desktops are loaded only with trusted software, and reminding users not to respond to e-mails from Nigerians with dubious business propositions. "With seven million systems in the DoD, think how many idiots there are bound to be," one Pentagon cybersecurity official says.* [54]

Operational Security (OPSEC) Concerns vs Network Security Concerns Regarding Social Media Use

OPSEC concerns regarding social media have almost clouded the discussion. While there are legitimate concerns, there are also many regulations covering OPSEC (not as many as cover network security, but enough). OPSEC is included in the user level information security training cited above, and is also a general requirement for all military personnel – and not just in regards to use of computers. DoD Manual 5205.02-M provides guidance on OPSEC. OPSEC is defined as:[55]

> *The OPSEC process is a systematic method used to identify, control, and protect information.*
>
> *Critical information is information about DoD activities, intentions, capabilities, or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technical advantage. Such information, if revealed*

to an adversary, may prevent or degrade mission accomplishment, cause loss of life, or damage friendly resources.

To assist in training OPSEC standards specifically regarding social media tools, the services have prepared brochures to guide the service member – and the family member – in what they should and should not say when using these capabilities.[56]

Continual emphasis on this aspect of the use of social media tools cannot be ignored and must be at the forefront of operator training. But, the fear of OPSEC violations cannot be the driving factor in denying access to social media services. It is the responsibility of commanders at all levels to train their employees and trust them enough to put this 'weapon' in their hands as much as they train them on all other weapons. And if violations occur, retraining and punishment may be required. The Israeli Army provides a good example (this Soldier's buddies will think twice about what they post on their Facebook page from now on):[57]

The Israeli military called off a raid in Palestinian territory after a soldier posted details, including the time and place, on social networking website Facebook.

The soldier described in a status update how his unit planned a "clean-up" arrest raid in a West Bank area, the radio station said. Facebook friends then reported him to military authorities.

The Israeli military spokeman's office issued a statement saying the soldier's actions could "undermine operational success and imperil forces."

It added that the soldier was sentenced to 10 days' imprisonment, his Combat certificate was revoked, and he was relieved from his battalion.

Social Media Use in the Department of Defense and other Federal Government Agencies

Over the past year, the use of social media services by the Public Affairs departments of the Office of the Secretary of Defense, the Chairman of the Joint Chiefs

of Staff, and the Army, Navy, Air Force, Marines and National Guard has increased exponentially. Most recently (early 2010) the Air Force found Twitter to be an effective tool in their earthquake response operations in Haiti; the Navy used Twitter and Facebook to keep service members, family, and the public informed during the Hawaiian tsunami and the earthquake in Chile, and the National Guard used Twitter and Facebook to inform the public of their rescue efforts during the recent devastating snowstorms in the northeastern United States. These social media tools are also being used to open a dialog with the public, though there is still work to be done. The Army periodically invites people to a discussion on Facebook regarding different military occupational specialties (MOS), and the DoD has a website titled “Open Government” inviting people to “JOIN THE CONVERSATION”.[58]

Use of social media tools on the GIG is now officially sanctioned. On February 25, 2010, Directive Type Memorandum (DTM) 09-026 was released. This document states that “The NIPRNET[59] shall be configured to provide access to Internet-based capabilities across all DoD Components”.[60] Jack Holt, Senior Strategist for Emerging Media, OSD, recently released another training tool, a poster called a ‘Safety Checklist’[61] to accompany the DTM, providing additional OPSEC guidance specifically for social networking sites, and a link to educational games[62] to aid in training on the use of these internet tools. DoD personnel and others who follow the daily actions in of the DoD are celebrating the increased openness this memorandum is mandating; while others are more wary of the implications of increased access to Facebook and Twitter from the workplace – concerns ranging from network security issues to OPSEC issues to simply ‘wasting government time’. This paper thus far has extensively detailed the

current regulations that cover network security and OPSEC issues – 'wasting government time' is covered in many personnel policies and is a leadership issue best addressed through appropriate channels.

The DTM also encourages DoD elements to register their social media sites so that the public will be able to distinguish those that are official from those that are not. These official sites will be linked off of the main portal of each of the different Services as well as the '*DoD Live'* portal[63]. As a point of reference, as of March 5, 2010, the DoD had 131 registered Facebook sites; the Army, 177; the Air Force 46; the Navy,150; and the Marines, 30.[64]

The Army[65] and the Marines[66] have recently released their Service specific version of the DTM – to specifically address their Soldiers and Marines; the Navy[67] is promising to issue one soon. Each of these documents, reiterating the DTM, emphasizes the user-level training required in order to properly educate the military members of the potential for OPSEC leaks, or of increased vulnerabilities to the GIG through successful phishing, malware, or Trojan attacks. None of these specifically emphasize to the network security administrators the need for increased diligence in protecting the GIG through proper network management practices – as stated earlier, there are many regulations that cover network management, and the addition of social media access does not change the overall IS and IA requirements. The Army memorandum specifically addresses user diligence: "All Army personnel have a personal and professional responsibility to ensure that no information that might place Soldiers in jeopardy or be of use to adversaries be posted to public Web sites".[68]

Only over time will it be determined if the policy outlined in the DTM and supplemental Service specific memorandum are adequate to address the various concerns regarding social media use on the GIG. Until then - the DTM is written, and as with all DoD policies, it is to be followed. And as with all DoD policies, this one will be reviewed, revised and re-released as required.

Current findings of increased risk to the GIG due to use of social media

A review of recent articles in leading Federal and commercial Information Technology and Information Security publications resulted in scarce discussion regarding increased vulnerability or security violations to the network through the use of social media tools. A popular belief is that the 'tiny URL' used in Twitter is a leading source of malware. One study of over 1 million URLs discovered that only 0.06% redirected to malicious content.[69] One 'risk' apparently unfounded.

Another study conducted by the Army found that "official Army Web sites violated operational security more than military bloggers".[70] This same report stated that resources were being "diverted from reviewing official sites by attention they have to give to Soldiers' blogs".[71]

> *Audits performed by the Army Risk Assessment Cell, found at least 1,813 violations of operational security on 878 official military Web sites and only 28 on 594 soldier blogs reviewed between January 2006 and January 2007.*

Wired magazine staff attorney Marcia Hoffman (who obtained the Army report) states: "It's clear that official Army Web sites are the real security problem, not blogs. Bloggers, on the whole, have been very careful and conscientious. It's a pretty major disparity".[72] One has to question, with reports such as these from the Army, why there is still such concern over individual soldiers' OPSEC on personal social media when the actual

problem is individual user adherence to the policies when under the auspices of their official military duties. Could it be that the punishment for violations for personal use are more severe than those under professional use?

Conclusion and Recommendations

Rules, regulations, policies, standards, specifications – all are created by people, by humans. A review of numerous articles, reports, regulations and interviews has shown that the biggest vulnerability in network security is the human in the loop. Even if information systems are automated to detect intrusions (which they are), it is the human that must ensure the most up-to-date version of the intrusion detection system is installed; it is the human that must check the logs and interpret them in order to understand and correct the vulnerabilities in the system. So, instead of reinforcing the opinion of the Pentagon cyber security official who believes there are a 'bunch of idiots out there'[73], efforts must focus on creating tools that are useable. Studies conducted at Carnegie Mellon University are pointing in that direction. Dr Lorrie F. Cranor, Director of Cylab Useable Privacy and Security states, "In order to develop tools that will be effective in combating these schemes (phishing), we first must know how and why people fall for them".[74] The same can be said regarding any aspect of network security – before we can be effective in combating these schemes, intrusions, insecurities, we must first understand why, in the face of numerous articles, reports, investigations, speakers, experts, salesmen and others – the human in the loop still decides to ignore the repeated warnings and education to properly utilize and maintain the GIG.

Implementing the 'easy' solution does not solve the problem – "The armed forces find it much easier to ban something than to educate its troops about responsible use".[75]

The DoD must:

- Continue training on both network security and OPSEC
- Continue partnering with industry to make security awareness and security tools more user friendly so they will be followed
- Continue reporting attacks – sharing information regarding attacks with others will only strengthen the defense of the network overall. Learn from each other mistakes
- Develop defense-in-depth techniques focusing more on protecting the data than on building a better wall to keep the cyber criminals out. Encrypt data so that only those authorized can obtain it, and teach users to not use the same password for each application and portal they use (one of the biggest vulnerabilities)
- Establish and enforce punishments for those network administrators who fail to properly perform their Information Security duties, and to those who provide information on official military web sites and social media sites as strongly and quickly as they are enforced to the individual service member on a personal social media site.

Information systems security starts at the beginning, with the education in our schools and our homes. Today's generation has grown up using computers, and today's generation will be the one to look to solve the vulnerability issues. The United States must increase education in the schools regarding cyber use, increase the interest in math and science for all students, and encourage young people to realize that computers do more than provide a great 'toy' to talk to your friends and play video games. DHS Secretary Napolitano discussed the need to hire 1,000 cyber security experts over the next three years to meet the nation's information security vulnerability challenges[76], and both she and the newly appointed White House Cyber security Coordinator are focusing on efforts to encourage the government, private sector, and citizens to all work together on these challenges. DHS is currently sponsoring a National Security Awareness Challenge to increase cyber security awareness and aid in cyber

education efforts.[77] As the public becomes more educated in the realities of cyber security, the efforts of the Department of Defense will be better supported from a more informed public and a more educated pool of recruits (both civilian and military) to fill positions in units at all levels.

ENDNOTES

[1] Deputy Secretary of Defense, "Directive-Type Memorandum (DTM) 09-26 – Responsible and Effective Use of Internet-based Capabilities", February 25, 2010, http://www.defense.gov/NEWS/DTM%2009-026.pdf (accessed on February 27, 2010).

[2] Doug Beizer, "Marines: Facebook is not for the Few Good Men", *Federal Computer Week*, August 4, 2009, http://fcw.com/Articles/2009/08/04/Marines-ban-social-networking.aspx (accessed on August 24, 2009).

[3] Jim Dao, "Military Web Policy 2.0", *AtWar blog (NYTimes.com),* October 3, 2009, http://atwar.blogs.nytimes.com/2009/10/03/military-web-policy-20/ (accessed on October 10, 2009).

[4] Examples of this negative public relations can be found at James Dao, "Leashing the Blogs of War", *AtWar blog (NYTimes.com),* September 8, 2009, http://atwar.blogs.nytimes.com/2009/09/08/leashing-the-blogs-of-war , and Chris Bronk, "Marines Social Media ban is bad for morale", *Federal Computer Week*, September 17, 2009, http://fcw.com/articles/2009/09/21/comment-chris-bronk-marine-ban.aspx?s=fcwdaily_180909 (accessed on October 10, 2009).

[5] Larry Shaughnessy, Barbara Starr and Pam Benson, "CIA, FBI push 'Facebook for Spies'", *CNN.com Technology*, September 5, 2008, http://www.cnn.com/2008/TECH/ptech/09/05/facebook.spies/index.html (accessed on April 5, 2010)

[6] According to the MilTech Solutions Office, an Army Organization, the milSuite application allows the professional 'DOD' community to share information amongst themselves that is only intended for the internal community. MilBook, which has reached 18,000 users since its inception in October 2009, is part of a suite of tools known as milSuite that also includes a blog and wiki. Official registration is required to access this portal, which is also password protected, thus it cannot substitute for commercial social media services for some communications requirements.

[7] Deputy Secretary of Defense, "Directive-Type Memorandum (DTM) 09-026 – Responsible and Effective use of Internet-based Capabilities", February 25, 2010, http://www.defense.gov/NEWS/DTM%2009-026.pdf (accessed on February 27, 2010).

[8] Department of the Army Memorandum, "Responsibly Use of Internet-based Capabilities", March 25, 2010.

[9] Larry Wortzel, "China's Cyber Offensive", *Asian Wall Street Journal*, November 2, 2009, http://online.wsj.com/article/SB10001424052748703399204574508413849779406.html (accessed on January 20, 2010).

[10] Ibid

[11] DODD 8500.01E, "Information Assurance", October 24, 2002

[12] Marcus H. Sachs, Director, SANS Internet Storm Center, "Cybersecurity: Emerging Trends, Vulnerabilities, and Challenges in Securing Federal Information Systems", *Testimony before the House Committee on Oversight and Government Reform, Sub Committee on Management, Organization and Procurement*, May 5, 2009.

[13] Katherine C. Den Bleyker, "The First Amendment vs Operational Security: Where should Milblogging Balance Lie", 2007, http://iplj.net/blog/wp-content/uploads/2009/09/Note-THE-FIRST-AMENDMENT-VERSUS-OPERATIONAL-SECURITY-WHERE-SHOULD-THE-MILBLOGGING-BALANCE-LIE1.pdf (accessed on March 2, 2010)

[14] Ibid

[15] Michele Tepper, "The rise of social software," *netWorker*, volume 7, number 3, pp. 18–23, 2003.

[16] Access acquired through log-in and password access of Common Access Card and restricted to Army personnel, https://www.kc.army.mil/milsuite

[17] AKO – Army Knowledge Online. DKO – Defense Knowledge Online. AKO provides the Army enterprise with email, directory services, portal, single sign on, blogs, file storage, instant messenger and chat. All members of the Active Duty, National Guard, Reserves, DA Civilian and select contractor workforce have an account which grants access to Army web assets, tools and services worldwide. In addition, retirees and family members are also entitled to accounts. All users can build pages, create file storage areas, and create and participate in discussion on the portal. Users can build custom access control lists for each piece of content they own to determine the audience allowed to see or use their content. As of this writing, AKO has 2.2 million registered users, and supports over 350K users logging in up to a million times a day as well as receiving and delivering on average 12 million emails daily, http://en.wikipedia.org/wiki/Army_Knowledge_Online, (accessed on April 7, 2010).

[18] President Barack Obama, Memorandum for Heads of Executive Departments and Agencies, January 21, 2009, http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government/, (accessed on December 15, 2009).

[19] Peter R. Orszag, Open Government Directive, December 8, 2009, http://www.whitehouse.gov/open/documents/open-government-directive, (accessed on February 27, 2010)

[20] Review conducted by author from February-April 2009

[21] This number refers to the National Guard Bureau, and does not reflect a total of the use of these tools in the separate 54 States and Territories that make up the National Guard, many which host their own sites.

[22] Gen Craig McKinley, "Why I Tweet….social networks transform the way we work", *Federal Times*, November 23, 2009, p 23, http://www.federaltimes.com/article/20091120/ADOP06/911200310/1040/ADOP06 (accessed on December 15, 2009)

[23] President George Bush, "National Strategy for Information Sharing", The White House, October 2007, http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html (accessed on March 1, 2010)

[24] Ibid, Introduction and Overview

[25] Department of Defense Information Sharing Strategy, prepared by the Information Sharing Executive Office of the Chief Information Officer, May 4, 2007, p iii

[26] United States Intelligence Community Information Sharing Strategy, February 22, 2008

[27] Department of Homeland Security Information Sharing Strategy, April 18, 2008

[28] Information Assurance Technology Analysis Center, "The DoD IA Policy Chart", IATAC website, http://iac.dtic.mil/iatac/ia_policychart.html, (accessed on March 1, 2010)

[29] Information Assurance Technology Analysis Center, "Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance", The Office for the Assistant Secretary of Defense for Networks and Information Integration / DOD Chief Information Officer, http://iase.disa.mil/policy-guidance/dasd_ciia__strategy_aug2009.pdf (accessed on March 1, 2010)

[30] USSTRATCOM is the DoD's Unified Combatant Command responsible for (among other area), space and cyber operations.

[31] Information Assurance Technology Analysis Center, "The DoD IA Policy Chart", IATAC website, http://iac.dtic.mil/iatac/ia_policychart.html, (accessed on March 1, 2010)

[32] Information Assurance Technology Analysis Center, "Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance", The Office for the Assistant Secretary of Defense for Networks and Information Integration / DOD Chief Information Officer, http://iase.disa.mil/policy-guidance/dasd_ciia__strategy_aug2009.pdf , p. v, (accessed on March 1, 2010)

[33] Department of the Army, "AR 25-1, Information Management / Information Assurance", March 23, 2009, http://www.army.mil/usapa/epubs/pdf/r25_2.pdf (accessed on March 1, 2010)

[34] Department of Defense, "DODD 8570.01, Information Assurance, Training and Workforce Management", Arpil 23, 2007, http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf (accessed on March 1, 2010)

[35] Department of the Army, "AR 25-1, Information Management / Information Assurance", March 23, 2009, http://www.army.mil/usapa/epubs/pdf/r25_2.pdf p. 1, (accessed on March 1, 2010)

[36] Assistant Secretary of Defense for Networks and Information Integration, Department of Defense Directive 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP), November 28, 2007

[37] U.S Code, Subchapter III of Chapter 35 of title 44, United States Code, "Federal Information Security Management Act (FISMA) of 2002", http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

[38] Ibid, § 3544 – Federal Agency responsibilities

[39] U.S Army Enterprise Solutions Competency Center, "Army Information Assurance (IA) Compliance Strategy and Reference Guide", http://escc.army.mil/doc/ESCC_0608_Flipbook_Green_IA_reprint.pdf (accessed on March 3, 2010)

[40] USAF Standard Desktop Configuration (SDC), June 2007, http://www.silicon.com/white-papers/client-system-hardware/2007/06/01/the-usaf-standard-desktop-configuration-sdc-60321882/ (accessed on April 6, 2010)

[41] Executive Office of the President, Office of Management and Budget, M-07-11, Implementation of Accepted Security Configurations for Windows Operating Systems, March 22, 2007.

[42] Ken Page, The Federal Desktop Core Configuration, White Paper, *Microsoft Corporation*, January 2008, http://www.microsoft.com/industry/government/solutions/FDCC/default.aspx#get_info, (accessed on March 3, 2010)

[43] OMB Mandate, March 22, 2007, accessed from http://www.microsoft.com/industry/government/solutions/FDCC/default.aspx#get_info (accessed on March 3, 2010)

[44] Amber Corrin, All-seeing security program spreading throughout DoD, Federal Computer Week, December 9, 2009, http://fcw.com/articles/2009/12/08/host-based-security-usaf-cyber-command.aspx (accessed on March 3, 2010)

[45] Angela Moscaritolo, "Military's ban of USB thumb drives highlights security risks", *SC Magazine,* November 20,2008, http://www.scmagazineus.com/militarys-ban-of-usb-thumb-drives-highlights-security-risks/article/121326/ (accessed on March 3, 2010)

[46] Bob Sullivan, "Military Thumb drives expose larger problem", *Red Tape Chronicles*, April 30, 2006, http://redtape.msnbc.com/2006/04/military_thumb_.html (accessed on March 3, 2010)

[47] Army Knowledge Online, On Cyber Patrol Portal, https://www.us.army.mil/suite/portal/index.jsp (password protected web site)

[48] Ibid

[49] Department of Defense Directive, 8570.01E, "Information Assurance Training, Certification and Workforce Development", Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer, August 23, 2007, http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf (accessed on March 3, 2010)

[50] Department of Defense 8570.01-M, “Information Assurance Workforce Improvement Program”, Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer”, February 25, 2010

[51] DoDD 8570.01, p 2

[52] DoD 8570.01-M, p 43-46

[53] IAVA – Information Assurance Vulnerability Alert. http://en.wikipedia.org/wiki/Information_Assurance_Vulnerability_Alert (accessed on April 10, 2010)

- An announcement of a computer application software or operating system vulnerability notification in the form of alerts, bulletins, and technical advisories identified by DoD-CERT, a division of the Joint Task Force-Global Network Operations. These selected vulnerabilities are the mandated baseline, or minimum configuration of all hosts residing on the GIG. JTF-GNO analyzes each vulnerability and determines if is necessary or beneficial to the Department of Defense to release it as an IAVA. Implementation of IAVA policy will help ensure that DoD Components take appropriate mitigating actions against vulnerabilities to avoid serious compromises to DoD computer system assets that would potentially degrade mission performance.
- The COCOMs, Services, and Agencies and field activities are required to implement vulnerability notifications in the form of alerts, bulletins, and technical advisories. USSTRATCOM has the authority to direct corrective actions, which may ultimately include disconnection of any enclave, or affected system on the enclave, not in compliance with the IAVA program directives and vulnerability response measures (i.e. communication tasking orders or messages). USSTRATCOM and JTF-GNO will coordinate with all affected organizations to determine operational impact to the DoD before instituting a disconnection.

[54] Noah Shachtman, “Spooks in the Machine: How The Pentagon Should Fight Cyber Spies”, *Progressive Policy Institute White Paper*, January 2010, http://www.progressivefix.com/spooks-in-the-machine-how-the-pentagon-should-fight-cyber-spies, (accessed on March 3, 2010)

[55] Department of Defense Manual 5205.02-M, “DoD Operations Security (OPSEC) Program Manual”, Undersecretary of Defense for Intelligence, November 3, 2008, p 12

[56] Navy Information Operations Command, “OPSEC, a guide for the family”, http://www.niocmd.navy.mil/main/highlights/family_brochure.pdf (accessed on March 4, 2010) and The Pentagon OPSEC Working Group, “OPSEC and Internet Safety”, http://www.au.af.mil/au/awc/awcgate/dod/blogbrochure.pdf (accessed on March 4, 2010)

[57] Allyn Fisher-Ilan, “Israeli Army nixes raid after Facebook leak – radio”, *Reuters Africa,* March 3, 2010, http://af.reuters.com/article/oddlyEnoughNews/idAFTRE6221V920100303 (accessed on March 3, 2010)

[58] DoD Open Government, Transparency, Participation, Collaboration, http://www.defense.gov/open/ (accessed on March 3, 2010)

[59] NIPRNET – Non-classified Internet Protocol Router Network

[60] Deputy Secretary of Defense, "DTM 09-026 – Responsible and Effective Use of Internet-based Capabilities", February 25, 2010, http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-026.pdf (accessed on March 4, 2010)

[61] Safety Checklist, http://www.ioss.gov/sns_safety_check.pdf, (accessed on March 4, 2010)

[62] OnLineGuard.gov, http://socialmedia.defense.gov/index.php/games/ (accessed on March 4, 2010)

[63] DOD Live, http://www.dodlive.mil/

[64] These figures obtained by counting the registered user on the main portal of each of the elements mentioned. Some of the sites registered on the DoD page are also registered on the portal page of the separate service, so there is some double counting.

[65] Department of the Army, Office of the Secretary of the Army Memorandum, "Responsible Use of Internet-based Capabilities", March 25, 2010.

[66] Amy McCullough, "Corps lifts ban on social networking sites", *Marine Corps Times,* March 31, 2010, http://www.marinecorpstimes.com/news/2010/03/mairine_socialnetworking_032910w/ (accessed on April 11, 2010), and MARADMIN 181/10, RESPONSIBLE AND EFFECTIVE USE OF INTERNET-BASED CAPABILITIES, March 29, 2010, http://www.usmc.mil/news/messages/Pages/MARADMIN181-10.aspx (accessed on April 11, 2010)

[67] Department of the Navy, Chief Information Officer, "The DON IT Resource", March 26, 2010, http//www.doncio.navy.mil/blog.aspx (accessed on April 11, 2010)

[68] Ibid, p 4

[69] Julien Sobrier, "Unlike popular belief, short links on Twitter aren't malicious", *Help Net Security*, March 31, 2010, http://www.net-security.org/article.php?id=1418 (accessed on April 11, 2010)

[70] Robert Weller, "Report: Official sites biggest security threat", *Army Times*, August 18m 2007, http://www.armytimes.com/news/2007/08/ap_militaryblogs_070818/ (accessed on January 10, 2010.

[71] Ibid

[72] Ibid

[73] Noah Shachtman, "Spooks in the Machine: How The Pentagon Should Fight Cyber Spies", *Progressive Policy Institute White Paper*, January 2010,

http://www.progressivefix.com/spooks-in-the-machine-how-the-pentagon-should-fight-cyber-spies, (accessed on March 3, 2010)

[74] Dr Lorrie F. Cranor, Julie S. Downs and Mandy B. Holbrook, "Decision Strategies and Susceptibility to Phishing", Article Abstract, *School of Computer Science Institute for Software Research*, 2006, http://works.bepress.com/lorrie_cranor/1/, (accessed on March 3, 2010)

[75] Shachtman, p 3

[76] Eric Chabow, "Napolitano seeks Private Sector Security Help", RSA Conference, March 3, 2010

[77] DHS, National Cyber Security Awareness Campaign Challenge, http://www.dhs.gov/files/cyber-awareness-campaign.shtm (accessed on March 4, 2010)